Deutscher Bundestag
13. Wahlperiode

Drucksache 13/5179

28. 06. 96

Kleine Anfrage

der Abgeordneten Ulla Jelpke, Wolfgang Bierstedt und der Gruppe der PDS

Staatliche Kontrolle kryptografischer Techniken

Bestimmte Computer-Software (z. B. „Pretty Good Privacy" – PGP) ermöglicht es Computerprogramme und -texte zu verschlüsseln. Computertexte können mit dieser sog. kryptografischen Software wie in einen Briefumschlag abgelegt werden. Unbefugte – wie z. B. die Rechner von Polizei und Geheimdiensten – sind anscheinend nicht imstande diese Verschlüsselungs-Codes zu knacken. So konnte in einem – von der Bundesregierung in ihrer Antwort auf eine Große Anfrage der SPD zur „organisierten Kriminalität in der Bundesrepublik Deutschland" – zitierten Beispielsfall unter Verwendung von Mailboxen verschlüsselte Daten „trotz Einbindung in- und ausländischer Spezialdienststellen ein Großteil der Daten bislang nicht entschlüsselt werden" (Drucksache 13/4942, S. 95). Strafprozessuale, polizeirechtliche oder Möglichkeiten nach dem Gesetz zu Artikel 10 Grundgesetz zur Telefon- bzw. Fax-Überwachung können so z. B. im E-Mail-Bereich weitgehend unterlaufen werden.

Die Bundesregierung hatte 1993 schon einmal eine derartige Genehmigungspflicht überdacht. Nachdem sich aber Wissenschaftlerinnen und Wissenschaftler und Vertreter der Industrie einig waren, daß eine derartige staatliche Kontrolle kryptografischer Technik jederzeit unterlaufen werden könnte, wurden diese Pläne der Bundesregierung bis heute zurückgestellt (Drucksache 13/4105).

In einer Antwort (Drucksache 13/1889, S. 3) antwortete die Bundesregierung auf eine entsprechende Frage der Fraktion BÜNDNIS 90/DIE GRÜNEN, Verschlüsselungsverbote könnten zwar unterlaufen werden, die Existenz einer derartigen staatlichen Kontrolle schrecke aber zumindest ab.

Die niederländische Regierung hatte ebenfalls bereits einen Gesetzentwurf zur staatlichen Kontrolle kryptografischer Techniken ins Parlament eingebracht. Nach massiver Kritik mußte dieser Gesetzentwurf aber wieder zurückgezogen werden.

Wir fragen die Bundesregierung:

1. Ist der Bundesregierung bekannt, in wie vielen – aufgrund welcher Delikte geführten – Ermittlungs- bzw. Strafverfahren

die Tätigkeit der Strafverfolgungsbehörden durch die Verwendung welcher kryptografischer Techniken behindert wurde?

2. Ist der Bundesregierung bekannt, in wie vielen Fällen es den Strafverfolgungsbehörden (bzw. den von ihnen beauftragten in- und ausländischen Spezialdiensten) nicht möglich war, welche dieser kryptografischen Techniken aufzuschlüsseln?

3. a) Ist der Bundesregierung bekannt, ob in- und ausländische Behörden bzw. Spezialdienste zur Entschlüsselung kryptografisch verschlüsselter Kommunikationsinhalte und Programme herangezogen wurden, und wenn ja, welche und in wie vielen Fällen?

   b) Welche Kosten sind hierbei entstanden?

4. Welche Sanktionsformen der Verschlüsselungstechnologie plant die Bundesregierung?

5. Auf wen (öffentliche Haushalte, Anbieter von Telekommunikationsdiensten, Kunden) kommen hinsichtlich eines Verbots von kryptografischen Techniken aus Sicht der Bundesregierung voraussichtlich welche Kosten zu?

6. a) Welche neuen Handlungsmöglichkeiten plant die Bundesregierung für die Verfassungsschutzämter, das Bundesamt für Sicherheit und Informationstechnik (BSI), das Zollkriminalamt, den BND, den MAD bzw. Amt für Nachrichtenwesen der Bundeswehr (ANBw) nach der Einführung einer staatlichen Kontrolle der Verschlüsselungstechnologie?

   b) Welche Rahmenbedingungen entnimmt die Bundesregierung in diesem Zusammenhang den Formulierungen des Artikel 10 des Grundgesetzes und dem Gesetz zu Artikel 10 Grundgesetz und welche Veränderungen dieser Regelungen plant sie ggf.?

   c) Welche dieser Behörden waren an den Vorbereitungen der Bundesregierung für einen entsprechenden Gesetzentwurf in welcher Form beteiligt?

7. a) Welche Kritikpunkte wurden 1993 aus der Wissenschaft bzw. von Vertreterinnen und Vertretern der Industrie an dem Gesetzentwurf der Bundesregierung geäußert?

   b) Wie steht die Bundesregierung heute zu den damals vorgebrachten Kritikpunkten?

   c) Ist die Bundesregierung der Ansicht, daß heute eine derartige staatliche Kontrolle kryptografischer Techniken mit vergleichsweise geringem Aufwand und technischem Wissen leicht unterlaufen werden könnte?

   d) Hält die Bundesregierung „Abschreckung" für eine ausreichende Begründung für die Kontrolle der Verschlüsselungs-Techniken?

8. a) Welche Kritikpunkte führten – nach Kenntnis der Bundesregierung – zur Rücknahme des niederländischen Gesetzentwurfes?

   b) Wurden diese Kritikpunkte bei den Planungen der Bundesregierung berücksichtigt?

   Wenn ja, wie?

   Wenn nein, warum nicht?

   c) In welchen anderen westeuropäischen Ländern, der USA bzw. Japan sind nach Erkenntnissen der Bundesregierung Gesetze welchen Inhalts zur staatlichen Kontrolle kryptografischer Techniken erlassen worden?

9. Ist der Datenschutzbeauftragte in die diesbezüglichen Planungen der Bundesregierung miteinbezogen worden?

   Wenn ja, was waren seine Anmerkungen und wie wurden sie berücksichtigt?

   Wenn nein, warum nicht?

Bonn, den 28. Juni 1996

Ulla Jelpke
Wolfgang Bierstedt
Dr. Gregor Gysi und Gruppe

Druck: Thenée Druck, 53113 Bonn, Telefon 91781-0
Vertrieb: Bundesanzeiger Verlagsgesellschaft mbH, Postfach 13 20, 53003 Bonn, Telefon (02 28) 3 82 08 40, Telefax (02 28) 3 82 08 44
ISSN 0722-8333